BF

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-040936

(43)Date of publication of application : 08.02.2002

(51)Int.Cl. G09C 1/00
G06F 17/60
H04L 9/32

(21)Application number : 2000-224462

(22)Date of filing : 25.07.2000

(71)Applicant : NTT ADVANCED TECHNOLOGY CORP

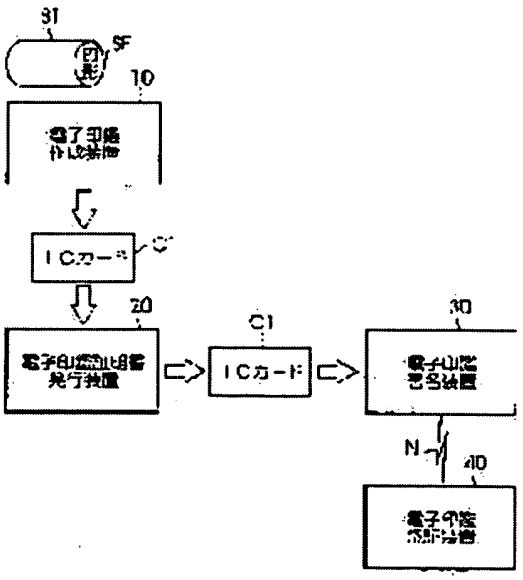
(72)Inventor : SHIRAISHI AKIRA

(54) ELECTRONIC SEAL GENERATION DEVICE, ELECTRONIC SEAL CERTIFICATE ISSUING DEVICE, ELECTRONIC SEAL SIGNING DEVICE, ELECTRONIC SEAL AUTHENTICATION DEVICE, AND SYSTEM AND METHOD FOR ELECTRONIC SIGNATURE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve convenience for a person to handle an electronic document by using authentication by an electronic signature and visual recognition by a conventional signature and an imprint of a seal together, to certify the truth of the electronic document.

SOLUTION: An electronic seal generation device 10 reads an imprint SF of a seal ST as information on the imprint and records it in an IC card C1 for the imprint information together with a public key. An electronic seal certificate issuing device 20 gives a certificate provided with a certification seal proving that the imprint information and the public key stored in the IC card C1 are genuine, and records the certificate in the IC card C1. An electronic seal signing device 30 attaches the imprint information to the electronic document and also creates a signed document provided with a signature of the electronic document holder. An electronic seal authentication device 40 judges the truth or falsehood of the electronic document based on the signed document and the certificate, and makes it possible to visually authenticate the document by displaying the imprint information attached to the signed document and the imprint information included in the certificate.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－40936
(P2002－40936A)
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G09C 1/00	640	G09C 1/00	640B 5B049
			640Z 5J104
G06F 17/60	512	G06F 17/60	512
H04L 9/32		H04L 9/00	673D

審査請求　未請求　請求項の数８　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－224462(P2000－224462)

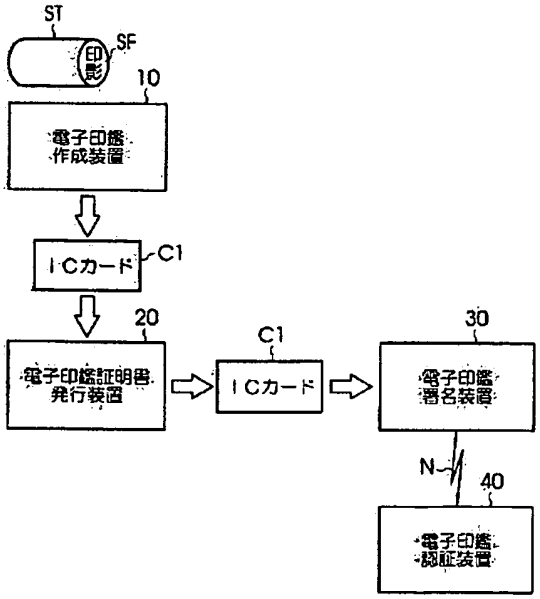
(22)出願日　平成12年７月25日(2000.7.25)

(71)出願人　000102739
エヌ・ティ・ティ・アドバンステクノロジ株式会社
東京都新宿区西新宿二丁目１番１号
(72)発明者　白石　旭
東京都新宿区西新宿二丁目１番１号　エヌ・ティ・ティ・アドバンステクノロジ株式会社内
(74)代理人　100064908
弁理士　志賀　正武

Ｆターム(参考)　5B049 AA05 AA06 EE09 FF01 GG00
5J104 AA07 AA09 AA16 EA04 KA01
KA16 LA03 LA06 NA02 NA35
NA37 NA38

(54)【発明の名称】　電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法

(57)【要約】
【課題】　電子文書の真偽を証明するに当たり、電子署名による認証と従来から用いられているサインや印影の目視による視認とを併用することによって、電子文書を取り扱う者の利便性を向上させる。
【解決手段】　電子印鑑作成装置１０は印鑑ＳＴの印影ＳＦを印影情報として読み取り印影情報用の公開鍵とともにＩＣカードＣ１に記録する。電子印鑑証明書発行装置２０は、ＩＣカードＣ１に記録されている印影情報及び公開鍵が真正であることを証明する証明印を付した証明書を発行してＩＣカードＣ１に記録する。電子印鑑署名装置３０は、電子文書に対して印影情報を添付するとともに、電子文書の保持者の署名を付した署名文書を作成する。電子印鑑認証装置４０は署名文書と証明書とに基づいて電子文書の真偽を判断し、署名文書に添付された印影情報と証明書に含まれる印影情報とを表示して目視による認証を可能とする。



1

【特許請求の範囲】

【請求項１】　印影を印影情報として読み取る印影読取部と、

前記印影情報用の公開鍵と秘密鍵とを対にして生成する印影情報用鍵生成部と、

前記印影情報と前記公開鍵とを対応づけるとともに、前記秘密鍵を付加した電子印鑑情報を作成する電子印鑑情報作成部と、

前記電子印鑑情報を電子印鑑に書き出す電子印鑑情報書出部とを具備することを特徴とする電子印鑑作成装置。

【請求項２】　少なくとも印影を示す印影情報と当該印影情報用に生成された公開鍵とが対応づけられて書き込まれている電子印鑑から、前記印影情報と前記公開鍵とを読み込む読込部と、

認証機関用の公開鍵と秘密鍵とを対にして生成する認証機関用鍵生成部と、

前記読込部から読み込んだ前記印影情報及び前記公開鍵に対して前記認証機関用の秘密鍵を用いて署名した証明印を付加した証明書を作成する証明書作成部とを具備することを特徴とする電子印鑑証明書発行装置。

【請求項３】　少なくとも認証機関用の秘密鍵を用いて署名が行われた印影を示す印影情報と前記印影情報用に作成された秘密鍵とが書き込まれている電子印鑑から前記印影情報と前記秘密鍵とを読み込む読込部と、

前記読込部から読み込んだ印影情報を電子文書に添付する印影添付部と、

前記印影が添付された電子文書に対して前記読込部から読み込んだ前記秘密鍵を用いて署名を行った署名文書を生成する署名部とを具備することを特徴とする電子印鑑署名装置。

【請求項４】　印影を示す印影情報が添付された電子文書に対して当該印影情報用の秘密鍵を用いて署名が行われた署名文書と、少なくとも前記印影情報と当該印影情報用に生成された公開鍵とが対応づけられてなる電子印鑑情報に対して認証機関用の秘密鍵を用いて署名が行われた署名印影情報とを読み込み、前記署名文書の署名と前記署名印影情報に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行う認証部と、

前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する印影表示部とを具備することを特徴とする電子印鑑認証装置。

【請求項５】　印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に対応づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出す電子印鑑作成装置と、

前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記

2

電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書に更新する印鑑証明書発行装置とを具備することを特徴とする電子署名システム。

【請求項６】　前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を生成する電子印鑑署名装置と、

前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する電子印鑑認証装置とを具備することを特徴とする請求項５記載の電子署名システム。

【請求項７】　印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に対応づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出すステップと、

前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書に更新するステップとを有することを特徴とする電子署名方法。

【請求項８】　前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を生成するステップと、

前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示するステップとを有することを特徴とする請求項７記載の電子署名方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、従来から用いられている印鑑の電子化を図った電子印鑑を作成する電子印鑑作成装置、従来から用いられている印鑑登録及び印鑑証明の電子化を図った電子印鑑証明書発行装置、文書に印鑑を捺印して行う署名の電子化を図った電子印鑑署名装置、及び文書の署名による文書の認証の電子化を図った電子印鑑認証装置、並びに電子署名システム及び電子署名方法に関する。

【０００２】

【従来の技術】近年、インターネットを代表としてコンピュータネットワーク化が進み、電子化された各種の文書データの授受が一般的に行われている。ネットワーク

を介して文書データの授受は誰でもいつでも迅速に行うことができるため、極めて利便性が高い。よって、文書データのみならず、画像や音声等の各種データがネットワークを介して授受されると予想されている。

【０００３】

【発明が解決しようとする課題】ところで、近年、電子政府プロジェクトの構成が予定されている。この電子政府プロジェクトは、各種申請書の電子化を図りインターネット等のネットワークを経由して各種申請手続きを行うものである。各種申請書の電子化が図られると、申請書に記載された情報にその個人の個性（例えば、筆跡等）が現れない。また、従来の窓口における対面業務と異なり、電子文書ではその電子文書が本人又は役所のものであるかの真偽が分からず、電子文書の内容が送信途中で改竄される虞がある等の危険性が指摘されている。

【０００４】かかる危険性を回避するため、上述した電子政府プロジェクトにおいては、認証機関を通じた本人であることを証明するための「電子署名」を導入し、インターネット等のネットワークを介して送受信される申請書の真正さを担保することにより危険性を回避する予定である。ここで、電子署名は、公開鍵と秘密鍵との２つの鍵を用いる公開鍵方式による暗号化技術を応用したものであり、本人のみが所有する秘密鍵を用いて電子文書に付した署名を、本人の公開鍵を用いて確認するものである。このような電子署名を用いることにより電子文書の内容が改竄されていないことと、その電子文書は本人により作成されたことの２点を証明することができる。よって、認証に関する技術は電子政府プロジェクトの基盤となるものであり、極めて重要な役割を果たすこととなる。

【０００５】しかしながら、旧来から法的効力を持つものとして利用されてきたサインや印影は、国民一般に広く浸透し、且つ慣習化しているため、電子文書の真偽の認証を電子的な署名のみによることは早急には国民一般に受け入れられないと考えられる。特に、サインや印影は本人及び窓口担当者の双方が同じものを容易に視認することができるものであるため、本人及び窓口担当者の双方が、本人が所有する印鑑を用いて捺印した申請書等の文書が窓口担当者へ渡され、又は役所が使用する印が捺印された文書が窓口担当者から本人へ渡されたことを確実に知ることができる。一方、電子署名の場合には、本人から窓口担当者へ又は窓口担当者から本人へ渡された文書には本人の電子署名が付されているか、又は役所が使用している署名であるかを確認することは極めて困難である。

【０００６】本発明は上記事情に鑑みてなされたものであり、電子文書の真偽を証明するに当たり、電子署名による認証と従来から用いられているサインや印影の目視による視認とを併用することによって、電子文書を取り扱う者の利便性を向上させることができる電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】上記課題を解決するために、本発明の電子印鑑作成装置は、印影を印影情報として読み取る印影読取部と、前記印影情報用の公開鍵と秘密鍵とを対にして生成する印影情報用鍵生成部と、前記印影情報と前記公開鍵とを対応づけるとともに、前記秘密鍵を付加した電子印鑑情報を作成する電子印鑑情報作成部と、前記電子印鑑情報を電子印鑑に書き出す電子印鑑情報書出部とを具備することを特徴としている。また、本発明の電子印鑑証明書発行装置は、少なくとも印影を示す印影情報と当該印影情報用に生成された公開鍵とが対応づけられて書き込まれている電子印鑑から、前記印影情報と前記公開鍵とを読み込む読込部と、認証機関用の公開鍵と秘密鍵とを対にして生成する認証機関用鍵生成部と、前記読込部から読み込んだ前記印影情報及び前記公開鍵に対して前記認証機関用の秘密鍵を用いて署名した証明印を付加した証明書を作成する証明書作成部とを具備することを特徴としている。また、本発明の電子印鑑署名装置は、少なくとも認証機関用の秘密鍵を用いて署名が行われた印影を示す印影情報と前記印影情報用に作成された秘密鍵とが書き込まれている電子印鑑から前記印影情報と前記秘密鍵とを読み込む読込部と、前記読込部から読み込んだ印影情報を電子文書に添付する印影添付部と、前記印影が添付された電子文書に対して前記読込部から読み込んだ前記秘密鍵を用いて署名を行った署名文書を生成する署名部とを具備することを特徴としている。また、本発明の電子印鑑認証装置は、印影を示す印影情報が添付された電子文書に対して当該印影情報用の秘密鍵を用いて署名が行われた署名文書と、少なくとも前記印影情報と当該印影情報用に生成された公開鍵とが対応づけられてなる電子印鑑情報に対して認証機関用の秘密鍵を用いて署名が行われた署名印影情報とを読み込み、前記署名文書の署名と前記署名印影情報に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行う認証部と、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する印影表示部とを具備することを特徴としている。本発明の電子署名システムは、印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に対応づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出す電子印鑑作成装置と、前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書

に更新する印鑑証明書発行装置とを具備することを特徴としている。また、本発明の電子署名システムは、前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を生成する電子印鑑署名装置と、前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する電子印鑑認証装置とを具備することを特徴としている。また、本発明の電子署名方法は、印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に対応づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出すステップと、前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書に更新するステップとを有することを特徴としている。また、前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を生成するステップと、前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示するステップを有することを特徴としている。

【０００８】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法について詳細に説明する。尚、以下の説明では印鑑の印影を用いる場合を例に挙げて説明する。しかしながら、本発明はサインの場合にも適用が可能である。つまり、本明細書で用いられる語句「印影」とは、印鑑の印影のみならずサイン等を含む意味である。

【０００９】〔電子署名システム〕図１は、本発明の一実施形態による電子署名システムの全体構成を示すブロック図である。以下、図面を参照して本発明の電子署名システムの構成及び動作の概要について説明する。図１に示したように、本発明の一実施形態による電子署名システムは、電子印鑑作成装置１０、電子印鑑証明書発行装置２０、電子印鑑署名装置３０、及び電子印鑑認証装置４０を含んで構成される。

【００１０】電子印鑑作成装置１０は、例えば印鑑ＳＴの販売店に配置され、印鑑ＳＴの印影ＳＦを印影情報として読み取るとともに印影情報用に対の公開鍵及び秘密鍵を生成する。そして、読み取った印影情報と作成した公開鍵とを対応づけるとともに生成した秘密鍵を付加した電子印鑑情報を作成して電子印鑑としてのＩＣカードＣ１に書き出す。電子印鑑作成装置１０の役割は、従来の印鑑作成に相当する。

【００１１】電子印鑑証明書発行装置２０は、区役所、市役所、第三者機関、その他の認証機関に配置され、ＩＣカードＣ１に記録されている電子印鑑情報がＩＣカードＣ１の保持者のものであることを証明する証明書を発行する。ＩＣカードＣ１の保持者は運転免許書やパスポート等の身分証明書とともにＩＣカードＣ１を公的機関に提出して証明書を発行してもらう。電子印鑑証明書発行装置２０は発行した証明書を既に記録されている印影情報及び公開鍵に代えてＩＣカードＣ１に書き出す。ＩＣカードＣ１に記録される証明書は従来の印鑑証明書に相当し、電子印鑑証明書発行装置２０の役割は、従来の印鑑登録と印鑑証明書の発行に相当する。このＩＣカードＣ１はいわば証明書入りの電子的な印鑑として利用される。

【００１２】電子印鑑署名装置３０は、例えばＩＣカードＣ１の保持者の自宅に配置されたパーソナルコンピュータによって実現され、ＩＣカードＣ１に書き込まれている証明書から印影情報を読み込み、読み込んだ印影情報をＩＣカードＣ１の保持者が作成した電子文書に対して添付する。また、ＩＣカードＣ１に記録されている秘密鍵を用いて印影情報が添付された電子文書に対する署名としての電子署名を生成する。このように、電子印鑑署名装置３０は、ＩＣカードＣ１の保持者が作成した電子文書に対して公的機関の認証を受けた証明書に含まれる印影情報を添付し、その保持者の電子署名を付した署名文書を作成する。電子印鑑署名装置３０の役割は、従来の文書への捺印に相当する。電子印鑑署名装置３０はインターネット等のネットワークＮを介して電子印鑑認証装置４０と接続され、署名文書とともに証明書を電子印鑑認証装置４０へ送信する。

【００１３】電子印鑑認証装置４０は、例えば区役所、市役所、その他の行政機関に配置され、ネットワークＮを介して送信されてきた証明書に含まれる印影情報用に生成された公開鍵を用いてネットワークＮを介して送信されてきた署名文書に添付された電子署名の真偽を判断することにより電子文書の認証を行う。また、電子印鑑認証装置４０は、署名文書中の電子文書に添付された印影情報と証明書に含まれる印影情報とをＣＲＴ（Cathod Ray Tube）等の表示装置に表示する。この表示装置に表示された印影情報を目視して行政機関の役人がその真偽を判断して電子文書を認証する。

【００１４】印鑑ＳＴの保持者が電子文書を作成する際

に、印鑑ＳＴの印影ＳＦをスキャナ等を用いて読み込み、この印影情報を添付した電子文書として作成すれば、行政機関の役人がその真偽を目視して判断することが可能であり、従来から行われている目視による認証をも行うことができると考えられる。しかしながら、単に印影情報を電子文書に添付するだけでは、電子文書に添付された印影情報は容易に流用及び改竄が可能である。従って、電子文書に添付された印影情報が改竄された場合にはその電子文書の真正を保証することができず、流用された場合には悪用される虞がある。

【００１５】これに対し、本発明の一実施形態による電子署名システムは、上述したように印影ＳＦの印影情報を電子署名の認証に利用される公開鍵と同様に、信用のおける認証機関が署名した証明書として発行してもらい、この証明書付きの印影情報を電子文書に添付している。これにより、電子署名で保証された文書の真正を、印影による目視によっても証明することができるようになり、これまで慣習となっていた印影による文書の真正の証明手段としての親和性を確保することができる。

【００１６】尚、以上説明した本発明の一実施形態による電子署名システムにおいては、電子印鑑作成装置１０が印鑑ＳＴの販売店に配置され、電子印鑑証明書発行装置２０は、区役所、市役所、第三者機関、その他の認証機関に配置され、各々が別々に設けられている場合を例に挙げて説明した。しかしながら、電子印鑑作成装置１０及び電子印鑑証明書発行装置２０をともに、例えば区役所、市役所等の行政機関に配置すれば、印鑑ＳＴと身分証明書とを行政機関に持っていくだけで、電子印鑑の作成、印鑑登録、及び印鑑証明書作成を行うことができる。

【００１７】以上、本発明の一実施形態による電子署名システムの全体構成について説明したが、次に電子署名システムに含まれる本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置について詳細に説明する。

【００１８】〔電子印鑑作成装置〕図２は、本発明の一実施形態による電子印鑑作成装置１０の構成を示すブロック図である。図２に示したように、電子印鑑作成装置１０は、印影読み取り部１２、鍵生成部１４、電子印鑑情報作成部１６、及び書き出し部１８を含んでなる。印影読み取り部１２は、例えばイメージスキャナ等によって実現され、印鑑ＳＴの印影ＳＦを印影情報Ｆ１として読み取る。鍵生成部１４は、印影情報Ｆ１用の公開鍵ＯＫ１と秘密鍵ＳＫ１とを対にして生成する。

【００１９】電子印鑑情報作成部１６は、印影読み取り部１２で読み取った印影情報Ｆ１と鍵生成部１４で生成された印影情報Ｆ１用の公開鍵ＯＫ１とを対応づけるとともに、鍵生成部１４で生成された印影情報Ｆ１用の秘密鍵ＳＫ１を付加した電子印鑑情報を作成する。書き出し部１８は、電子印鑑情報作成部１６で作成された電子印鑑情報をＩＣカードＣ１へ書き出す。以上の処理によって電子印鑑としてのＩＣカードＣ１が作成される。

尚、図２においては、印鑑ＳＴの印影ＳＦを読み取る場合を例に挙げて説明したが、印影ＳＦに代えて手書きのサインを印影情報とした電子印鑑情報を作成する場合にも適用することができる。

【００２０】〔電子印鑑証明書発行装置〕次に、本発明の一実施形態による電子印鑑証明書発行装置２０について詳細に説明する。図３は、本発明の一実施形態による電子印鑑証明書発行装置２０の構成を示すブロック図である。尚、図３においては、説明の便宜のためＩＣカードＣ１を２つ図示しているが、これらは物としては同一であり内部に記憶される情報のみが異なる。

【００２１】図３に示したように、本発明の一実施形態による電子印鑑証明書発行装置２０は、入出力部２２、鍵生成部２４、情報入力部２６、及び証明書作成部２８を含んでなる。入出力部２２は、電子印鑑としてのＩＣカードＣ１に対して任意の情報の読み込み、書き出し、及び更新ができる。この入出力部２２は読込部を含んでなす。鍵生成部２４は、ＩＣカードＣ１に記憶されている公開鍵ＯＫ１と印影情報Ｆ１とが、印鑑ＳＴの保持者のものであることを証明する証明印Ｓ１を生成するために用いる認証機関用の一対の公開鍵ＯＫ２と秘密鍵ＳＫ２とを生成する。

【００２２】この公開鍵ＯＫ２と秘密鍵ＳＫ２とはＩＣカードＣ２に書き出される。尚、本実施形態においては公開鍵ＯＫ２と秘密鍵ＳＫ２とがＩＣカードＣ２に書き出される場合を例に挙げて説明するが、必ずしもＩＣカードＣ２に書き出す必要はなく、他の記録媒体（例えば、フレキシブルディスク、ハードディスク、光磁気ディスク、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ等）に書き出すようにしても良い。また、公開鍵ＯＫ２は例えばインターネット等のネットワークを介して何人も入手することが可能である。

【００２３】上記証明印Ｓ１は一種の電子署名であり、鍵生成部２４が生成した秘密鍵ＳＫ２を用いて生成される。上述したように、公開鍵ＯＫ２は何人も入手することができるため何人も証明印Ｓ１の内容を見ることができるが、秘密鍵ＳＫ２が公開されていないため、例えその内容を見ることができたとしても証明印Ｓ１を作成することはできない。情報入力部２６は、例えばキーボード等により実現され、証明書の有効期限等を示す証明書情報Ｐ１を入力する。

【００２４】証明書作成部２８は、秘密鍵ＳＫ２を用いて署名した証明印Ｓ１を作成し、入出力部２２を介してＩＣカードＣ１から読み込んだ公開鍵ＯＫ１、印影情報Ｆ１、及び証明書情報Ｐ１に対して作成した証明印Ｓ１を付した証明書ＣＲを作成する。ここで、証明書ＣＲ中の公開鍵ＯＫ１及び印影情報Ｆ１は秘密鍵ＳＫ２を用いて署名した証明印Ｓ１が付加されており、これは署名印

影情報に相当するものである。この証明書ＣＲは入出力部２２を介してＩＣカードＣ１に書き出される。尚、このとき、入出力部２２は、先に記録されていた公開鍵ＯＫ１及び印影情報Ｆ１を証明書ＣＲに更新する。以上の処理によって証明書入りの電子的な印鑑が作成される。

【００２５】〔電子印鑑署名装置〕次に、本発明の一実施形態による電子印鑑署名装置３０について詳細に説明する。図４は、本発明の一実施形態による電子印鑑署名装置３０の構成を示すブロック図である。図４において、ＩＣカードＣ１は図３に示した電子印鑑証明書発行装置２０が発行した証明書ＣＲが記録されたＩＣカードである。

【００２６】図４に示したように、本発明の一実施形態による電子印鑑署名装置３０は、情報読み込み部３２、印影添付部３４、署名部３６、及び通信部３８を含んでなる。情報読み込み部３２は、ＩＣカードＣ１に記録されている証明書ＣＲ及び印影情報用の秘密鍵ＳＫ１を読み込む。印影添付部３４は、ＩＣカードＣ１の保持者が別途作成した電子文書Ｄに対して、証明書ＣＲに含まれる印影情報Ｆ１を添付する。

【００２７】署名部３６は、秘密鍵ＳＫ１を用いて電子文書Ｄの作成者の署名を作成し、印影情報Ｆ１が添付された電子文書Ｄに付加した署名文書ＳＤを作成する。通信部３８は、署名部３６が作成した署名文書を証明書ＣＲとともにインターネット等のネットワークＮへ送出する。以上の処理によって、ＩＣカードＣ１に記録された印影情報Ｆ１が添付された電子文書Ｄに、ＩＣカードＣ１の保持者の署名が付加された署名文書ＳＤが証明書ＣＲとともにネットワークを介して送信される。

【００２８】〔電子印鑑認証装置〕次に、本発明の一実施形態による電子印鑑認証装置４０について詳細に説明する。図５は、本発明の一実施形態による電子印鑑認証装置４０の構成を示すブロック図である。図５に示したように、電子印鑑認証装置４０にはネットワークＮを介して署名文書ＳＤと証明書ＣＲとが送信されてくる。かかる署名文書ＳＤ及び証明書ＣＲにより認証を行うために、電子印鑑認証装置４０は、通信部４２、認証部４４、及び印影表示部４６を備える。尚、図５においては、証明書ＣＲが署名文書ＳＤとともにネットワークＮを介して送信されてくる様子を示すとともに、証明書ＣＲ中のどの情報が認証に用いられるかを明確化するために、証明書ＣＲを２つ図示している。

【００２９】通信部４２は、ネットワークＮを介して授受される各種情報の通信制御を行う。認証部４４は、証明書ＣＲ中に含まれる公開鍵ＯＫ１を用いて電子署名Ｓ２を含む署名文書ＳＤが真正のものであるか否かの認証を行う。つまり、署名文書ＳＤに含まれる電子署名Ｓ２は、図４を用いて説明したようにＩＣカードＣ１に含まれる秘密鍵ＳＫ１によって作成されたものであるため、公開鍵ＯＫ１を用いれば電子署名Ｓ２の内容を確認することができ、よって電子署名Ｓ２の真偽を判断することによって、電子文書Ｄが真正のものであるか否かを認証することができる。印影表示部４６は、電子文書Ｄに添付されている印影情報Ｆ１と、証明書証明書ＣＲに含まれる印影情報をＣＲＴ等の表示装置に表示する。

【００３０】このように、電子印鑑認証装置４０は、認証部４４によって電子文書Ｄに付された電子署名Ｓ２の真偽によって電子文書Ｄが真正のものであるか否かを判断している。また、印影表示部４６によって電子文書Ｄに付された印影情報Ｆ１と証明書ＣＲに含まれる印影情報Ｆ１とを表示している。従って、電子文書Ｄが真正のものであるか否かの認証を行う際に、電子署名を用いて機械的に行うとともに、従来から行われている視認による認証を行うことができる。尚、印影表示部４６が電子文書Ｄに添付されている印影情報Ｆ１を表示する際には、電子文書Ｄに添付されている印影情報Ｆ１のみを表示しても良く、印影情報Ｆ１が付された状態での電子文書Ｄを表示するようにしても良い。

【００３１】〔電子署名方法〕以上、本発明の一実施形態による電子署名システムを構成する本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置について説明したが、次に電子署名システムの動作、つまり電子署名方法について詳細に説明する。

【００３２】まず、電子印鑑としてのＩＣカードＣ１を作成する場合には印鑑の販売店へ出向き印鑑ＳＴを選択する。そして、電子印鑑作成装置１０によって選択した印鑑ＳＴの印影ＳＦを読み取らせる。読み取られた印影情報Ｆ１は鍵生成部１４で生成された公開鍵ＯＫ１と対応づけられ、更に鍵生成部１４で生成された秘密鍵ＳＫ１が付加されて電子印鑑情報としてＩＣカードＣ１に書き出される。このようにして電子印鑑としてのＩＣカードＣ１が生成されたので、選択した印鑑ＳＴと生成したＩＣカードＣ１との代金を支払って購入する。

【００３３】ＩＣカードＣ１の保持者はＩＣカードＣ１と身分証明書とを持参して認証機関へ出向き、認証機関の窓口担当者にＩＣカードＣ１と身分証明書を差し出し、身分証明書によって窓口担当者に本人であることの確認をしてもらった上で、ＩＣカードＣ１内に証明書ＣＲを作成してもらう。電子印鑑証明書発行装置２０にＩＣカードＣ１が挿入されると、入出力部２２は、ＩＣカードＣ１から公開鍵ＯＫ１及び印影情報Ｆ１を読み込む。また、情報入力部２６からは有効期限等の証明書情報Ｐ１が入力される。

【００３４】証明書作成部２８は、鍵生成部２４が生成した秘密鍵ＳＫ２を用いて署名した証明印Ｓ１を作成し、入出力部２２を介してＩＣカードＣ１から読み込んだ公開鍵ＯＫ１、印影情報Ｆ１、及び証明書情報Ｐ１に対して作成した証明印Ｓ１を付した証明書ＣＲを作成する。この証明書ＣＲは入出力部２２を介してＩＣカード

Ｃ１に書き出され、先に記憶されている公開鍵ＯＫ１及び印影情報Ｆ１の更新がなされる。尚、証明書ＣＲには電子印鑑証明書発行装置２０の鍵生成部２４で生成された秘密鍵ＳＫ２を用いて作成された証明印Ｓ１が付されている。よって、証明印Ｓ１の内容を見ることはできるが、例えば印影情報Ｆ１を取り替えて偽の証明書ＣＲを作成することはできない。以上の処理を終えたＩＣカードＣ１はＩＣカードＣ１の保持者に身分証明書とともに返却される。

【００３５】ＩＣカードＣ１の保持者が自ら作成した電子印鑑を用いて捺印する場合には、ＩＣカードＣ１を電子印鑑署名装置３０に差し込む。ＩＣカードＣ１の保持者が印影情報Ｆ１を添付する電子文書Ｄを指定すると、ＩＣカードＣ１から証明書ＣＲに含まれる印影情報Ｆ１が読み込まれ、印影添付部３４が指定された電子文書Ｄに印影情報Ｆ１が添付される。次に、ＩＣカードＣ１から印影情報Ｆ１用に生成された秘密鍵ＳＫ１が読み込まれ、署名部３６がこの秘密鍵ＳＫ１を用いて電子署名Ｓ２を作成し、印影情報Ｆ１が付された電子文書Ｄに電子署名Ｓ２を付した署名文書ＳＤを作成する。

【００３６】この電子文書ＳＤは、ＩＣカードＣ１の保持者の秘密鍵ＳＫ１を用いて作成された電子署名Ｓ２が付されており、例え第三者がその内容を見ることはできても、秘密鍵ＳＫ１は、ＩＣカードＣ１内に格納されているため、ＩＣカードＣ１の保持者以外の者が電子署名Ｓ２と同一の電子署名を作成することはできない。よって、電子文書Ｄや印影情報Ｆ１の内容が改竄して電子署名Ｓ２と同一の電子署名を付した署名文書ＳＤを作成することはできない。従って、電子署名Ｓ２によって電子文書Ｄの真正さを担保することができる。

【００３７】ＩＣカードＣ１の保持者が作成した署名文書ＳＤを行政機関等に送信する場合には、保持者は署名文書ＳＤの送信指示を行う。かかる送信指示がなされると、署名文書ＳＤとともに証明書ＣＲがネットワークに送信される。署名文書ＳＤと証明書ＣＲとは別個に送信される訳ではなく一対にして送信される。署名文書ＳＤと証明書ＣＲとがネットワークＮを介して送信されてくると、電子署名Ｓ２が添付された電子文書Ｄが真正のものであるか否かが認証部４４によって判断されるとともに、印影表示部４６によって電子文書Ｄに付された印影情報Ｆ１と証明書ＣＲに含まれる印影情報Ｆ１とが表示される。従って、電子文書Ｄが真正のものであるか否かの認証を行う際に、電子署名を用いて機械的に行うとともに、従来から行われている視認による認証を行うことができる。

【００３８】以上、本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法について説明したが、本発明は上記実施形態に制限されることはなく、本発明の範囲内において

自由に変更が可能である。例えば、上記実施形態においては、電子印鑑認証装置４０が備える印影表示部４６によって電子文書Ｄに付された印影情報Ｆ１と証明書ＣＲに含まれる印影情報Ｆ１とを単に表示するだけであったが、電子文書Ｄに付された印影情報Ｆ１と証明書ＣＲに含まれる印影情報Ｆ１とのパターンが一致するか否かを判断する判断部を設けて目視による認証を自動化してもよい。更に、ＩＣカードＣ１に記録される印影情報Ｆ１を圧縮して記録に要する容量の低減を図ってもよい。尚、かかる場合には圧縮された印影情報Ｆ１の目視が必要となる電子印鑑署名装置３０及び電子印鑑認証装置４０に圧縮された印影情報Ｆ１を伸長して復元する復元部を設ける必要がある。

【００３９】

【発明の効果】以上、説明したように、本発明によれば、電子署名による電子文書の真正の認証と、電子文書に添付された印影によって文書の真正の認証とを並行して行うことができるという効果がある。また、電子文書に添付される印影情報は、電子文書に添付される電子署名を作成する際に利用される公開鍵とともに認証機関の認証を受けたものであり、この認証機関の認証を受けた証明書を用いて電子文書に添付された印影情報が真正のものであるか否かが判断される。よって、仮に電子文書に添付された印影情報が偽造されて別の印影情報が添付されていたとしても、電子文書に添付された印影情報と証明書に含まれる印影情報とが異なるため、偽造を知ることが可能になるという効果がある。

【図面の簡単な説明】

【図１】　本発明の一実施形態による電子署名システムの全体構成を示すブロック図である。

【図２】　本発明の一実施形態による電子印鑑作成装置１０の構成を示すブロック図である。

【図３】　本発明の一実施形態による電子印鑑証明書発行装置２０の構成を示すブロック図である。

【図４】　本発明の一実施形態による電子印鑑署名装置３０の構成を示すブロック図である。

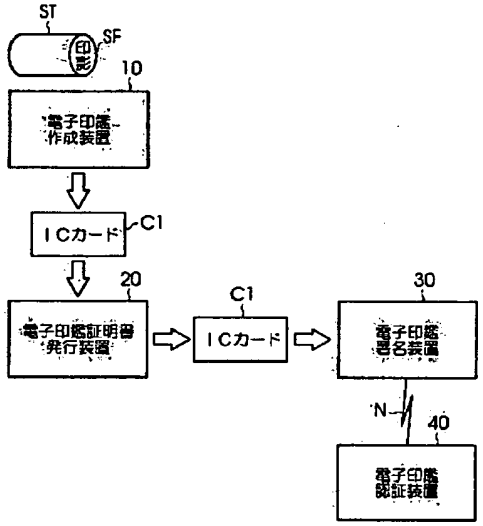
【図５】　本発明の一実施形態による電子印鑑認証装置４０の構成を示すブロック図である。

【符号の説明】

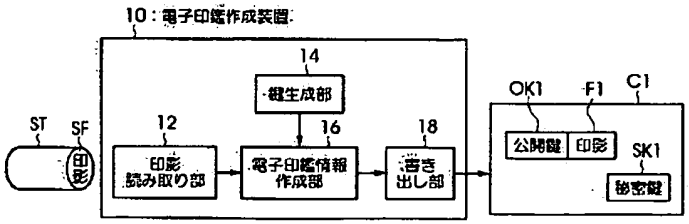
１０　電子印鑑作成装置
１２　印影読み取り部（印影読取部）
１４　鍵生成部（印影情報用鍵生成部）
１６　電子印鑑情報作成部
１８　書き出し部（電子印鑑情報書出部）
２０　電子印鑑証明書発行装置
２２　入出力部（読込部）
２４　鍵生成部（認証機関用鍵生成部）
２８　証明書作成部
３０　電子印鑑署名装置
３２　情報読み込み部（読込部）

３４	印影添付部	＊Ｆ１	印影情報
３６	署名部	ＯＫ１	印影情報用の公開鍵
４０	電子印鑑認証装置	ＯＫ２	認証機関用の公開鍵
４４	認証部	ＳＦ	印影
４６	印影表示部	ＳＫ１	印影情報用の秘密鍵
Ｃ１	ＩＣカード（電子印加）	ＳＫ２	認証機関用の秘密鍵
ＣＲ	証明書	＊	

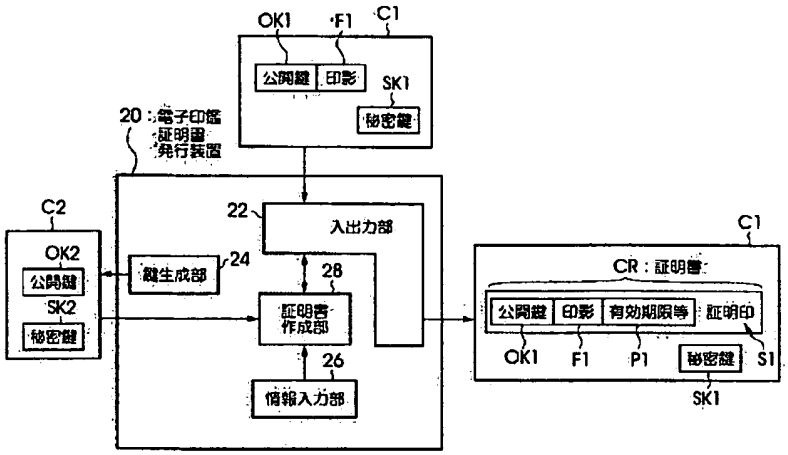
【図１】



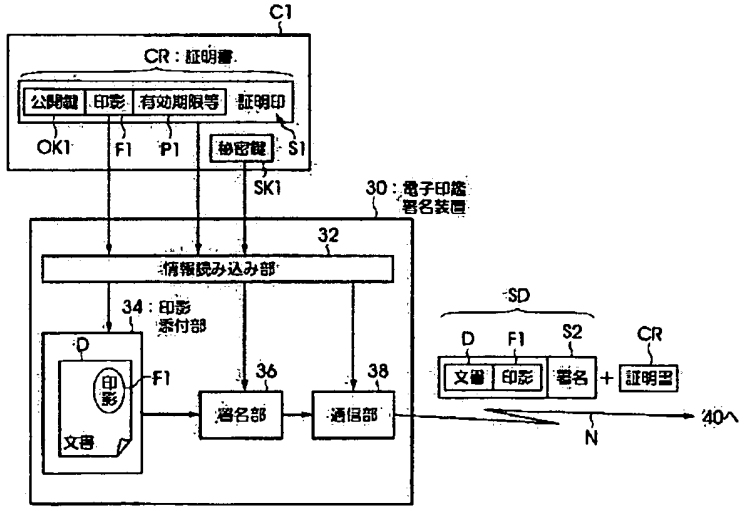
【図２】



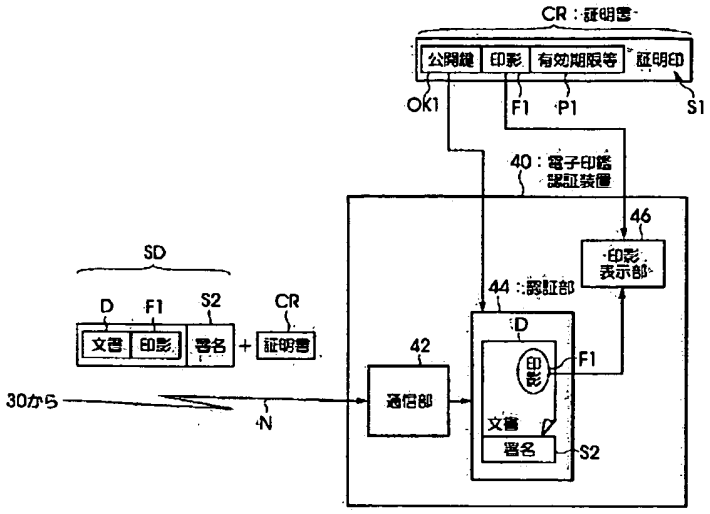
【図3】


OK1
F1
C1
公開鍵
印影
SK1
秘密鍵
20：電子印鑑
証明書
発行装置
C2
OK2
公開鍵
SK2
秘密鍵
22
入出力部
鍵生成部
24
28
証明書
作成部
26
情報入力部
C1
CR：証明書
公開鍵
印影
有効期限等
証明印
OK1
F1
P1
秘密鍵
S1
SK1

【図4】


C1
CR：証明書
公開鍵
印影
有効期限等
証明印
OK1
F1
P1
秘密鍵
S1
SK1
30：電子印鑑
署名装置
32
情報読み込み部
34：印影
添付部
D
印影
文書
F1
36
署名部
38
通信部
SD
D
F1
S2
CR
文書
印影
署名
+
証明書
N
40へ

【図５】


CR：証明書
公開鍵
印影
有効期限等
証明印
OK1
F1
P1
S1
40：電子印鑑認証装置
46
印影表示部
44：認証部
SD
D
F1
S2
CR
文書
印影
署名
証明書
42
通信部
30から
N
D
印影
F1
文書
署名
S2